UNITED STATES PATENT AND TRADEMARK OFFICE

A

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/067,319	02/07/2002	Swati Deshmukh	19903.0016	7037

23517   7590   08/12/2005

SWIDLER BERLIN LLP
3000 K STREET, NW
BOX IP
WASHINGTON, DC 20007

EXAMINER
SIMMONS, JIM

ART UNIT	PAPER NUMBER
2141	

DATE MAILED: 08/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
	10/067,319	DESHMUKH ET AL.
Office Action Summary	Examiner	Art Unit	
	James J. Simmons	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>07 February 2002</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-48</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-48</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>07 February 2002</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-48 are presented for examination.

Claim Objections

2.   Claim 8 is objected to under 37 CFR 1.75(c), as being of improper dependent form for

failing to further limit the subject matter of a previous claim. Applicant is required to cancel the

claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the

claim(s) in independent form. Examiner asserts that claim 8 expresses the same limitation as

expressed in parent claim 3.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
> in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
> patent by another filed in the United States before the invention by the applicant for patent, except that an
> international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this
> subsection of an application filed in the United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English language.

4.   Claims 1-8, 17-24, and 33-40 are rejected under 35 U.S.C. 102(e) as being anticipated

over Ackroyd (US 2003/0131256).

       a. As per claim 1, Ackroyd discloses a method of reporting malware events comprising

the steps of:

              detecting a malware event (Abstract);

determining the level of the detected malware event (p. 0027-0029; wherein

thresholds are levels of a detected malware event);

comparing the level of the detected malware event to an event trigger threshold

(p. 0027-0029); and

transmitting a notification of the detected malware event, based on the comparison of the

level of the detected malware event to the event trigger threshold (Fig. 1; policy organizing

server 32; p. 0011; p. 0025-0029).

b. As per claim 2, Ackroyd discloses the claimed invention as described above and

furthermore teaches detecting the malware event using a malware scanner (p. 0011; p. 0031-

0032)

c. As per claim 3, Ackroyd discloses the claimed invention as described above and

furthermore teaches that the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a

missing log file, detection of a malware, or failure of a response to a malware (p. 0025).

d. As per claim 4, Ackroyd discloses the claimed invention as described above and

furthermore teaches the malware event has a plurality of levels (Fig. 1, p. 0027-0029; wherein

thresholds are levels of a detected malware event).

e. As per claim 5, Ackroyd discloses the claimed invention as described above and

furthermore teaches the malware event comprises one of:

Informational malware events requiring no operator intervention; warning

malware events that indicate a process failure; minor malware events that require

attention, but are not events that could lead to loss of data; major malware events that

need operator attention; critical malware events that need operator attention; critical

malware events that need immediate operator attention and could lead to loss of data if

not corrected (p. 0027-0029; p. 0032; wherein the determination of whether or not

operator intervention is necessary is inherent of the ability to determine whether or not

the number of malware detections is significant.)

f. As per claim 6, Ackroyd discloses the claimed invention as described above and

furthermore teaches the malware event comprises one of a plurality of levels (p. 0027-0029; p.

0032; wherein trigger threshold can be set to a plurality of levels such as 0.1 percent of

computers detecting malware or 10 percent of computers detected malware).

g. As per claim 7, Ackroyd discloses the claimed invention as described above and

furthermore teaches the event trigger threshold comprises one of:

Informational malware events requiring no operator intervention; warning malware

events that indicate a process failure; minor malware events that require attention, but are not

events that could lead to loss of data; major malware events that need operator attention; critical

malware events that need operator attention; critical malware events that need immediate

operator attention and could lead to loss of data if not corrected (p. 0027-0029; p. 0032).

h. As per claim 8, Ackroyd discloses the claimed invention as described above and

furthermore teaches that the malware event comprises at least one of:

completion of a malware scan, a process failure relating to malware scanning, a missing

log file, detection of a malware, or failure of a response to a malware (p. 0025).

i. As per claims 17-24 and 33-40, claims are rejected because the have similar limitations

as claims 1-8; therefore, they are rejected under the same rationale.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth
> in section 102 of this title, if the differences between the subject matter sought to be patented and the prior
> art are such that the subject matter as a whole would have been obvious at the time the invention was made
> to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

6.   Claims 9-16, 25-32, and 41-48 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Ackroyd (US 2003/0131256) in view of Moore et al. (2003/0120947).

a. As per claim 9, Ackroyd discloses the claimed invention as described above. Ackroyd

does not explicitly teach the transmitting step comprises steps of:

          transmitting the notification of the detected malware event in real-time, if the

level of the detected malware event is greater than or equal to the event trigger threshold;

and

          transmitting the notification of the detected malware event in real-time, if the

level of the detected malware event is greater than or equal to the event trigger threshold;

and

          transmitting the notification of the detected malware event eventually, if the level

of the detected malware event is less than the event trigger threshold.

However, Moore teaches of the described transmitting steps (p. 0034; wherein malware

found actions may include sending message to system administrator immediately or after a

delayed period).   It would have been obvious to one of ordinary skill in the art at the time the

invention was made to incorporate the malware found transmitting actions of Moore into the

system of Ackroyd, since the field of inventions for both Ackroyd and Moore pertain to malware

detection and handling in a networked environment, and since it is desirable to reduce network

traffic by selectively transmitting based on the level of detected malware (Ackroyd, p. 0011)

b. As per claim 10, the Ackroyd-Moore system discloses the claimed invention as

described above and Ackroyd furthermore teaches the malware event has one of a plurality of

levels (Fig. 1, p. 0027-0029; wherein thresholds are levels of a detected malware event).

c. As per claim 11, the Ackroyd-Moore system discloses the claimed invention as

described above and furthermore teaches the malware event comprises one of:

Informational malware events requiring no operator intervention; warning

malware events that indicate a process failure; minor malware events that require

attention, but are not events that could lead to loss of data; major malware events that

need operator attention; critical malware events that need operator attention; critical

malware events that need immediate operator attention and could lead to loss of data if

not corrected (p. 0027-0029; p. 0032; wherein the determination of whether or not

operator intervention is necessary is inherent of the ability to determine whether or not

the number of malware detections is significant.)

d. As per claim 12, the Ackroyd-Moore system discloses the claimed invention as

described above and Ackroyd furthermore teaches the event trigger threshold comprises one of a

plurality of levels (p. 0027-0029; p. 0032; wherein trigger threshold can be set to a plurality of

levels such as 0.1 percent of computers detecting malware or 10 percent of computers detected

malware).

e. As per claim 13, the Ackroyd-Moore system discloses the claimed invention as described above and Ackroyd furthermore teaches the event trigger threshold comprises one of:

Informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected (p. 0027-0029; p. 0032).

f. As per claim 14, the Ackroyd-Moore system discloses the claimed invention as described above and Ackroyd furthermore teaches that the malware event comprises at least one of: completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of a malware, or failure of a response to a malware (p. 0025).

g. As per claim 15, the Ackroyd-Moore system discloses the claimed invention as described above and Ackroyd furthermore teaches detecting the malware event using a malware scanner (p. 0011; p. 0031-0032).

h. As per claim 16, the Ackroyd-Moore system discloses the claimed invention as described above and Moore furthermore teaches transmitting an alert to an administrator indicating occurrence of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold (p. 0034; wherein the network administrator is issued a warning message).

i. As per claims 25-32 and 41-48, claims are rejected because the have similar limitations as claims 9-16; therefore, they are rejected under the same rationale.

Conclusion

7.   The prior art made of record and not relied upon is considered pertinent to applicant's

discloser.

a. Halperin et al. (US 2002/0194490) disclose a method of virus containment in computer

networks.

b. Hinchliffe et al. (US 2003/0023866) disclose centrally managed malware scanning.

c. Suuronon et al. (US 2003/0145228) disclose providing virus protection on a gateway.

d. Nachenberg et al. (US 2003/0088680) disclose temporal access control for computer

virus prevention.

8.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to James J. Simmons whose telephone number is (517) 272-8668.

The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be

reached on 571-272-3880. The fax phone number for the organization where this application or proceeding is

assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER